UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/735,876	12/13/2000	Thomas J. Parenty	20906-000210	9347

20350 7590 06/07/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
NORRIS, TREMAYNE M	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 06/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/735,876	PARENTY, THOMAS J.	
	Examiner	Art Unit	
	Tremayne M. Norris	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claim 28 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Line 16 of claim 8 describes a system under control of the encryption server system that installs the JAVA "decryption applet on the client system". It is unclear as to where within the specification that this feature is taught. It is understood that this limitation is present when performed under control of the client system.

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-30 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Trademarks such as "Java", "Netscape Navigator", and "Internet Explorer" should not be used as limitations in the claims.

Claim Objections

5. Claim 8 objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 8 restates what was stated in claim 7 regarding the first and second entries with respect to the symmetric key and cipher text document.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1,3,7-15,17,18,20,21,23-30 rejected under 35 U.S.C. 102(e) as being anticipated by Sasaki et al (US pat 6,351,536).

Regarding claim 1, Sasaki teaches a method of encrypting a shared document, comprising:

under control of an encryption server system,

generating a ECC public/private key pair for the encryption server system (col.10 lines 14-17);

under control of a client system,

requesting a Java® encryption applet from the encryption server system (col.3 lines 22-26; col.9 lines 25-31) ;

requesting an encryption server system EEC public key from the encryption server system (col.10 lines 14-17);

under the control of the encryption server system,

transmitting the Java® encryption applet to the client system over a secure channel (col.9 lines 40-44);

transmitting the encryption server system EEC public key to the client system over a secure channel (col.9 lines 40-44);

under control of a client system,

receiving the Java® encryption applet from the encryption server system over a secure channel (col.9 lines 25-31);

receiving the encryption server system EEC public key from the encryption server system over a secure channel (col.10 lines 14-17);

installing the Java® encryption applet on the client system (col.10 lines 5-9);

running the Java® encryption applet on the client system to generate a Triple DES symmetric key (col.10 lines 5-9);

encrypting a clear text document with the Triple DES symmetric key, thereby creating a cipher text document (col.9 lines 32-34);

creating a relationship between the cipher text document and the Triple DES symmetric key (col.2 lines 14-17);

encrypting Triple DES symmetric key with the encryption server EEC public key, thereby creating an encrypted Triple DES symmetric key (col.7 lines 50-59) ;

creating a relationship between the cipher text document and the encrypted Triple DES symmetric key (col.2 lines 14-17; col.7 lines 50-59);

transmitting the cipher text document to the encryption server system (col.9 lines 32-35);

transmitting the encrypted Triple DES symmetric key to the encryption server system (col.7 lines 57-59);

transmitting the relationship between the cipher text document and the encrypted Triple DES symmetric key to the encryption server system (col.7 lines 12-35);

under the control of the encryption server system,

storing the cipher text document in a storage medium ;

storing the encrypted Triple DES symmetric key in a storage medium (col.7 lines 25-29); and

storing the relationship between the cipher text document and the encrypted Triple DES symmetric key in a storage medium (col.17 lines 18-23).

Regarding claim 3, Sasaki teaches the Java encryption applet is installed on a browser (col.2 line 64 thru col.3 line 4)

Regarding claim 7, Sasaki teaches the steps of

under the control of the encryption server system,

storing the relationship between the cipher text document and the encrypted Triple DES symmetric key by making a first and a second entry in a con-elation table, the first entry representing the encrypted Triple DES symmetric key (col.20 lines 52-55), and the second entry representing the cipher text document (col.20 lines 48-51).

Regarding claim 8, Sasaki teaches wherein the first entry is the encrypted Triple DES symmetric key and the second entry is the cipher text document (col.20 lines 48-51).

Regarding claim 9, Sasaki teaches the first entry is a pointer to the encrypted Triple DES symmetric key and the second entry is a pointer to the cipher text document (col.20 lines 48-51).

Regarding claim 10, Sasaki teaches the steps of:

under the control of the encryption server system,

decrypting the encrypted Triple DES symmetric key with the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key (col.7 line 66 thru col.8 line 3);

decrypting the cipher text document with the decrypted Triple DES symmetric key, thereby creating a clear text document (col.8 lines 3-6); and,

storing the clear text document on the encryption server system (col.7 lines 6-7; col.17 lines 42-43).

Regarding claim 11, Sasaki teaches comprising the steps of

under the control of the encryption server system,

using the first entry in the correlation table to retrieve the encrypted Triple DES symmetric key (col.8 lines 35-39);

decrypting the encrypted Triple DES symmetric key using the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key (col.7 line 66 thru col.8 line 3);

decrypting the cipher text document with the decrypted Triple DES symmetric key, thereby creating a clear text document (col.8 lines 3-6);

storing the clear text document on a storage medium (col.7 lines 6-7; col.17 lines 42-43); and

making a third entry in the correlation table, thereby creating a relationship between the cipher text document, the clear text document and the encrypted Triple DES symmetric key (col.20 lines 35-60)

Regarding claim 12, Sasaki teaches the third entry is the clear text document (col.20 lines 35-40).

Regarding claim 13, Sasaki teaches the third entry is a pointer to the clear text document (col.20 lines 35-40).

Regarding claim 14, Sasaki teaches the steps of:

under control of the client system,

requesting the cipher text document from the server (col.13 lines 55-57) ;

under control of the encryption server system,

using the first entry in the correlation table to retrieve the encrypted Triple DES symmetric key (col.8 lines 35-39);

decrypting the Triple DES symmetric key using the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key (col.7 line 66 thru col.8 line 3);

inserting the Triple DES symmetric key into a Java decryption applet (col.13 lines 58-67);

sending the Java decryption applet to the client system over a secure channel (col.14 lines 20-26);

sending the cipher text document to the client system (col.13 lines 55-57);

under control of the client system,

installing the Java decryption applet on the client system (col.14 lines 20-31); and,

decrypting the cipher text document using the Java decryption applet, thereby creating a clear text document (col.13 lines 64-67).

Regarding claim 17, Sasaki teaches the steps of

under control of the client system,

requesting the clear text document from the server;

under control of the encryption server system,

generating a Triple DES symmetric key (col.13 lines 39-43);

encrypting the clear text document with the Triple DES symmetric key, thereby creating a cipher text document (col.13 lines 47-49);

inserting the Triple DES symmetric key into a Java decryption applet (col.13 lines 58-67);

sending the Java decryption applet to the client system over a secure channel (col.14 lines 20-26);

sending the cipher text document to the client system (col.13 lines 55-57);

under control of the client system,

installing the Java decryption applet on the client system (col.14 lines 20-31); and,

decrypting the cipher text document using the Java decryption applet, thereby creating a clear text document (col.13 lines 64-67).

Claims 15,18, and 21 are substantially equivalent to claim 3, therefore claims 15,18, and 21 are rejected because of similar rationale.

Claim 20 is substantially equivalent to claim 17, therefore claim 20 is rejected because of similar rationale.

Claim 23 is substantially equivalent to claim 10, therefore claim 23 is rejected because of similar rationale.

Claims 24 and 25 are substantially equivalent to claim 1, therefore claims 24 and 25 are rejected because of similar rationale.

Claim 26 is substantially equivalent to claim 7, therefore claim 26 is rejected because of similar rationale.

Claim 27 is substantially equivalent to claim 11, therefore claim 27 is rejected because of similar rationale.

Claim 28 is substantially equivalent to claim 14, therefore claim 28 is rejected because of similar rationale.

Claim 29 is substantially equivalent to claim 17, therefore claim 29 is rejected because of similar rationale.

Claim 30 is substantially equivalent to a combination of claims 1,10,14, and 17 as described below, therefore claim 30 is rejected because of similar rationale.

An encryption system for shared documents, comprising:

an encryption server system and a client system;

the encryption server system,

generating a ECC public/private key pair for the encryption server system (claim 1);

transmitting the Java encryption applet to the client system over a secure channel (claim 1);

transmitting the encryption server system EEC public key to the client system over a secure channel (claim 1);

storing the cipher text document in a storage medium (claim 1);

storing the encrypted Triple DES symmetric key in a storage medium (claim 1);

storing the relationship created between the cipher text document and the encrypted Triple DES symmetric key in a storage medium (claim 1);

using the first entry in the correlation table to retrieve the encrypted Triple DES symmetric key (claim 14);

decrypting the Triple DES symmetric key using the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key (claim 14);

inserting the encrypted Triple DES symmetric key into a Java decryption applet (claim 14);

sending the Java decryption applet to the client system over a secure channel (claim 14);

sending the cipher text document to the client system (claim 14);

decrypting the encrypted Triple DES symmetric key using the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key (claim 10);

sending the cipher text document to the client system (claim 14);

generating a Triple DES symmetric key (claim 17);

encrypting the clear text document with the Triple DES symmetric key, thereby creating a cipher text document (claim 17);

a client system,

requesting a Java encryption applet from the encryption server system (claim 1);

requesting an encryption server system EEC public key from the encryption server system (claim 1);

receiving the Java encryption applet from encryption server system over a secure connection (claim 1);

receiving an encryption server system EEC public key from the encryption server system over a secure channel (claim 1);

installing the Java encryption applet on the client system (claim 1);

running the Java encryption applet on the client system to generate a Triple DES symmetric key (claim 1);

encrypting a clear text document with the Triple DES symmetric key, thereby creating a cipher text document (claim 1);

creating a relationship between the cipher text document and the Triple DES symmetric key (claim 1);

encrypting Triple DES symmetric key with the encryption server EEC public key, thereby creating an encrypted Triple DES symmetric key (claim 1);

creating a relationship between the cipher text document and the encrypted Triple DES symmetric key (claim 1);

transmitting the document encrypted with the Triple DES symmetric key from the client system to the encryption server system (claim 1);

transmitting the Triple DES symmetric key encrypted with the encryption server system EEC public key from the client system to the encryption server system (claim 1);

transmitting the relationship between the cipher text document and the encrypted Triple DES symmetric key to the encryption server system (claim 1);

requesting the cipher text document from the server (claim 14);

installing the Java decryption applet on the client system (claim 14); and,

decrypting the cipher text document using the Java decryption applet, thereby creating a clear text document (claim 14); and,

requesting the clear text document from the server (claim 17).

Claim Rejections - 35 USC § 103

Claims 2,5,6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasaki (US pat 6,351,536).

Regarding claims 2,5, and 6, the examiner takes official notice that the use of various network transfer protocols are notoriously well known in the data processing arts. It would have been obvious to one of ordinary skill in the art at the time of the invention to use such protocols in order to carry requests from a browser to a web server and to transport pages from web servers back to the requesting browser in a fast and secure fashion.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (703) 305-8045. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 305-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

May 28, 2004

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137